IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	10/597,496
Applicant	:	Hajime Maekawa, *et al.*
Filed	:	July 27, 2006
Title	:	INFORMATION PROCESSING DEVICE, SERVER, COMMUNICATION SYSTEM, ADDRESS DECISION METHOD, ADDRESS MODIFICATION METHOD, AND PROGRAM
Conf. No.	:	1885
TC/A.U.	:	TBD
Examiner	:	TBD
Customer No.	:	52054
Docket No.	:	40442

Mail Stop Petitions
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION TO MAKE SPECIAL &
STATEMENT & DISCUSSION REGARDING PREEXAMINATION SEARCH AND MOST RELEVANT UNCOVERED REFERENCES IN SUPPORT

Sir:

Applicant hereby submits this Petition to Make Special to request an Acceleration of the Examination of this application, under 37 CFR § 1.102(d) according to MPEP §708.02(VIII). Please charge Deposit Account No. 16-0820, Order No. 40442 in the amount of $130.00 for the petition fee under 37 CFR § 1.17(h), and Applicant provides the attached Statement and Discussion. Note that copies of cited references are not included, according to current practice, but are listed on an already filed IDS.

STATEMENT & DISCUSSION REGARDING PREEXAMINATION SEARCH, AND MOST RELEVANT UNCOVERED REFERENCES IN SUPPORT

PREEXAMINATION SEARCH

A patentability search was conducted by the Japanese Office of the International Bureau of the co-pending application, PCT/JP2005/000565, the front page of which is attached hereto as Attachment 1. The Preliminary Report on Patentability is attached hereto as Attachment 2. An accurate English translation of the Reasoned Statement under PCT Rule 43, 2.1 is attached hereto as Attachment 2A. Note that claims 3-5, 7-13, 16-29, 32-38, 39-41, 44-49, and 51-53 of the PCT application were indicated as being both novel and unobvious.

The claims of the U.S. application in this case, as amended in the first Preliminary Amendment of July 28, 2006, are an accurate translation of the claims in the attached PCT application, and thus the international search is applicable to those claims, as the claims in the U.S. application are of similar scope to the claims of the PCT application. We note that the amendments provided in the Preliminary Amendment of July 28, 2006, were for the purpose of correcting grammar, putting the claims into a form more common for U.S. practice, or for the purpose of correcting translation errors, and thus the amendments did not impact the scope of the claims.

Filed with this petition is a second Preliminary Amendment that cancels the claims that were indicated as being not novel and/or obvious by the Preliminary Report. Furthermore, of the claims remaining in the co-filed Preliminary Amendment (claims 4, 5, 8, 9-16, 20-21, 24-28, 32, 36, and 37 remain) independent claims 4, 20, and 32 have been indicated as being novel and unobvious by the Preliminary Report. The remaining claims in the Preliminary Amendment have been amended to depend on one of these independent claims, and/or to include additional limitations, but all are thus novel and unobvious due to their dependency upon the independent claims.

Accordingly, the claims of the second Preliminary Amendment, filed with this petition, are patentable over the relevant references discovered in the International Search as discussed in more detail below.

DISCUSSION OF MOST RELEVANT REFERENCES

The references that were cited in the attached Preliminary Report on Patentability (attachment 2) were cited and filed with a previously filed IDS. A corrected machine translation of the Japanese patent reference (JP 2001-268125, hereinafter reference 2), and accurate English translations of the two additional references (Umemoto, hereinafter reference 1 and Yamada, hereinafter reference 3) are attached to this petition as attachments 3, 4, and 5, respectively. The current claims, as presented in the Preliminary Amendment, are patentable over these references for the following reasons.

Claim 4, the first independent claim, recites an "information-processing device for a communication source that performs tunnel communication with a communication destination device, comprising:"

> a judgment part for determining whether the information-processing device is a caller or a callee in the tunnel communication; and
>
> an address determination part for determining an address used for the communication target data according to the determination by the judgment part.

The second independent claim, claim 20, recites a similar judgment part at lines 2-3, and recites a server comprising an address determination part that determines:

> a first address of the first information-processing device and a second address of the second information-processing device, wherein both addresses are used for encapsulated communication target data in the tunnel communication performed between the first information-processing device and the second information-processing device according to the determination by the judgment part[.]

Finally, independent claim 32 recites a method of determining an address with the steps of

> determining which of a first information-processing device and a second information-processing device performing tunnel communication is a caller or a callee; and

determining an address used for encapsulated communication target data in the tunnel communication performed between the first information-processing device and the second information-processing device according to the determination by the judging step.

The cited references 1, 2, and 3 do not teach any "address determination part" that determines an address according to the determination by the judgment part (i.e., whether the information-processing device is a caller or a callee in the tunnel communication) as required by the current independent claims of the application.

Instead, reference 1 (see attachment 4) clearly teaches that a database of IPv6 addresses are assigned to respective users on the server side, and when a tunnel is set, static routing is performed with respect to the connected users (see page 2, last full paragraph). There is no teaching of any judgment part, as recited in the claims, and thus there can be no teaching of an address determination part that determines an address according to the determination by the judgment part. Similarly, there is no firs determination step of "determining which of a first information-processing device and a second information-processing device performing tunnel communication is a caller or a callee" and thus there can be no second determination step of determining an address based on such a determination.

Similarly, reference 2 (see attachment 3) teaches that a new conversion table is generated by NAT when a collision is detected, done in a manner that the addresses that collided no longer conflict (see, e.g., paragraphs 0012-0013 of the reference). However, yet again, there is no teaching of any "judgment part" or first determination step as required by the claims, and thus there can be no determining of addresses as required by the claims.

Finally, reference 3 (see attachment 5) teaches that private addresses are pooled beforehand and used by the IPsec device to overcome address duplication and thus avoid collision (see the section IP Address Operation on page 6 of the reference). There is, yet again, no teaching of the "judgment part" or first determination step as required by the claims, which determines "whether the information-processing device is a caller or a callee" and thus there can be no determining of addresses as required by the claims.

Consequently, claims 4, 20, and 32 are all patentable over the cited references, which coincides with the conclusion of the International Bureau Preliminary Report. The remaining

claims are dependent, directly or indirectly, on one of the independent claims discussed above, and are thus patentable over the references discovered in the international search based on that dependency.

Thus, because a search Japanese office of the International Bureau has found that the current claims are patentable over the most relevant references, and as discussed in more detail above, the claims are therefore patentable over the prior art.

If there are any additional fees resulting from this communication, please charge the same to our Deposit Account No. 16-0820, our Order No. 40442.

Respectfully submitted,

PEARNE & GORDON LLP

By: /Robert F. Bodi/
Robert F. Bodi, Reg. No. 48540

1801 East 9th Street
Suite 1200
Cleveland, Ohio 44114-3108
(216) 579-1700

Date: August 24, 2006

Attachment 1

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年8 月11 日 (11.08.2005)

PCT

(10) 国際公開番号
WO 2005/074208 A1

(51) 国際特許分類[7]: H04L 12/56

(21) 国際出願番号: PCT/JP2005/000565

(22) 国際出願日: 2005 年1 月19 日 (19.01.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-022902 2004 年1 月30 日 (30.01.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 前川 肇 (MAEKAWA, Hajime). 池田 巧 (IKEDA, Takumi).

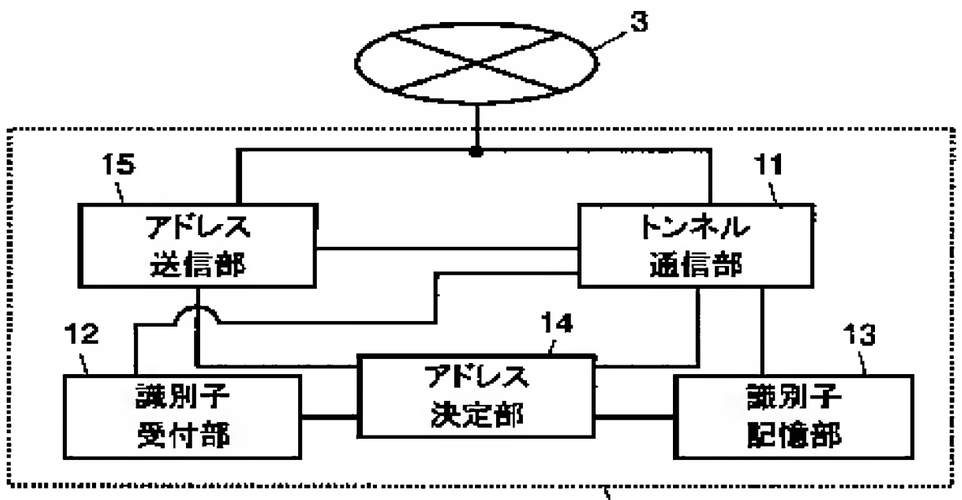
(74) 代理人: 岩橋 文雄， 外(IWAHASHI, Fumio et al.); 〒5718501 大阪府門真市大字門真１００６番地 松下電器産業株式会社内 Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE,

[続葉有]

(54) Title: INFORMATION PROCESSING DEVICE, SERVER, COMMUNICATION SYSTEM, ADDRESS DECISION METHOD, ADDRESS MODIFICATION METHOD, AND PROGRAM

(54) 発明の名称: 情報処理装置、サーバ、通信システム、アドレス決定方法、アドレス変更方法およびプログラム



第１の情報処理装置１

15... ADDRESS TRANSMISSION UNIT
11... TUNNEL COMMUNICATION UNIT
12... IDENTIFIER RECEPTION UNIT
14... ADDRESS DECISION UNIT
13... IDENTIFIER STORAGE UNIT
1... FIRST INFORMATION PROCESSING DEVICE

(57) Abstract: A first information processing device (1) of a communication source performing tunnel communication with a device of a communication destination includes: a tunnel communication unit (11) for encapsulating data to be communicated and performing tunnel communication; an identifier reception unit (12) for receiving a communication destination device identifier for identifying the device of the communication destination; an identifier storage unit (13) for storing the communication source device identifier for identifying the first information processing device (1); and an address decision unit (14) for deciding the address used for the data to be communicated, according to the communication destination device identifier and the communication source device identifier. With this configuration, it is possible to decide the address used for the data to be encapsulated to be communicated in the tunnel communication.

(57) 要約: 通信先の装置とトンネル通信を行う通信元の第１の情報処理装置（１）であって、通信対象のデータをカプセル化してトンネル通信を行うトンネル通信部（１１）と、通信先の装置を識別する通信先装置識別子を受け付ける識別子受付部（１２）と、第１の情報処理装置（１）を識別する通信元装置識別子を記憶している識別子記憶部（１３）と、通信先装置識別子と、通信元装置識

[続葉有]

WO 2005/074208 A1

Attachment 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/000565

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Jitsuyo Shinan Toroku Koho	1996-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	Hajime UMEMOTO, "BSD de My Server o Tsukuro!, Dynamic Tunnel", BSD magazine 2000 No.5, Ascii Corp., 31 December, 2000 (31.12.00), pages 115 to 117, Fig. 1	1,6,14,15, 30,31,42,43 2
X	JP 2001-268125 A (Nippon Telegraph And Telephone Corp.), 28 September, 2001 (28.09.01), Par. Nos. [0012] to [0013]; Figs. 2 to 4	38,50
Y A	Eiji YAMADA, "Solution Unyo·Kokoga Point! Dai 1 Kai, Internet VPN Unyo-Zenpen-Pilot Test to Sekkei no Point", N+1 NETWORK, Softbank Publishing Inc., Vol.2, No.12, 01 December, 2002 (01.12.02), pages 130 to 135, 'IP Address no Unyo' Ran	2 3-5,7-13, 16-29,32-37, 39-41,44-49, 51-53

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 March, 2005 (22.03.05)	05 April, 2005 (05.04.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

Attachment 2

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2005/000565

JP 2001-268125 A	2001.09.28	(Family: none)

Attachment 2

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ２００５／０００５６５

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ１２／５６

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ１２／５６

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　　１９２２－１９９６
日本国公開実用新案公報　１９７１－２００５
日本国登録実用新案公報　１９９４－２００５
日本国実用新案登録公報　１９９６－２００５

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	梅本　肇，ＢＳＤでMy　Ｓｅｒｖｅｒを作ろう！，ダイナミックトンネル，ＢＳＤ ｍａｇａｚｉｎｅ　２０００　Ｎｏ．５，株式会社アスキー，２０００．１２．３１，ｐ．１１５－１１７，図１	1, 6, 14, 15, 30, 31, 42, 43 2
X	ＪＰ　２００１－２６８１２５　Ａ（日本電信電話株式会社）２００１．０９．２８，第【００１２】－【００１３】段落，【図２】－【図４】	38, 50
Y	山田英史，ソリューション運用・ここがポイント！第１回，イン	2

☒ Ｃ欄の続きにも文献が列挙されている。

☒ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２２．０３．２００５	05.04.2005

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	清水　稔	５Ｘ	８５２５
	電話番号　０３－３５８１－１１０１　内線　３５５５		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００４年１月）

Attachment 2

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ２００５／０００５６５

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ターネットＶＰＮ運用―前編―パイロットテストと設計のポイント，Ｎ＋Ｉ　ＮＥＴＷＯＲＫ，ソフトバンクパブリッシング株式会社，第２巻，第１２号，２００２年１２月１日，ｐ．１３０－１３５，「ＩＰアドレスの運用」欄	3-5, 7-13, 16-29, 32-37, 39-41, 44-49, 51-53

Attachment 2

国際調査報告 パテントファミリーに関する情報	国際出願番号　ＰＣＴ／ＪＰ２００５／０００５６５

JP 2001-268125 A　2001.09.28　　ファミリーなし

Attachment 2A

[This is a translation of ISR Box V of Attachment 2]

Box V Reasoned statement under PCT rule 43, 2.1 with regard to novelty, inventive step or industrial applicability and references and explanations supporting the reasons.

1. Statement

Novelty (N)	Claims	2-5, 7-13, 16-29, 32-37, 39-41, 44-49, 51-53	novel
		1, 6, 14, 15, 30, 31, 38, 42, 43, 50	not novel
Inventive Step (IS)	Claims	3-5, 7-13, 16-29, 32-37, 39-41, 44-49, 51-53	unobvious
		1, 2, 6, 14, 15, 30, 31, 38, 42, 43, 50	obvious
Industrial Applicability (IA)	Claims	1-53	industrially applicable
			not applicable

2. References and explanations

Reference 1: Hajime Umemoto, Title: "BSD de My Server wo tsukurou"(Let's make My Server with BSD!), Dinamic Tonnel, BSD magazine 2000 No. 5, Aski Co., Ltd., December 31, 2000, p. 115-117, Fig. 1

Reference 2: Japanese patent application publication No. 2001-268125 A (NIPPON TELEGR & TELEPH CORP (NTT)), publication date: September 28, 2001, paragraphs[0012]-[0013], Figs. 2-4

Reference 3: Eiji Yamada, Title: "Solution unyou/kokoga point! Dai 1 kai, Internet VPN Unyo-Zenpan-Pailot Test to Sekkei no Point" (Solution Operation/This is the point! First part, Internet VPN operation – first part-pilot tests and points of designing), Volume 2, Issue 12, December 1, 2002, P 130-135, "IP address unyou"(IP address operation)

The inventions in claims 1, 6, `4, 15, 30, 31, 42, 43 are described in the reference 1 cited in the international search report, and therefore are not novel or unobvious.

The inventions in claim 2 are not novel because of the references 1 and 3 cited in the international search report. The reference 3 describes pooling addresses which should be assigned as private addresses, and it is easy for the skilled in the art to select the "assigning Ipv6 address" of the reference 1 from several predetermined addresses.

The inventions in claims 3-5, 7-13, 16-29, 32-37, 39-41, 44-49, 51-53 are not described in any of the references cited in the international search report and therefore unobvious.

Attachment 3 (Reference 2)

JP2001-268125 (Petition to Make Special Reference 2)

1.This document has been substantially translated by computer with some corrections added thereto. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

[Claim(s)]
[Claim 1] The VPN selection connection gateway characterized by to have a Twice-NAT conversion means to change the transmitting agency address and the transmission place address based on the connection request from a user terminal, and a virtual routing means function as two or more routers by which it became independent logically, in the selection connection gateway which has a means to function as a HTTP server, and a means to function as a DHCP server.
[Claim 2] When it asks the DSN server of a connection place network, duplication of an IP address is detected from the reply to this inquiry based on the connection request from a user terminal and there is duplication Change the IP address in the end of a connection tip into an intact IP address, and the this changed IP address is registered into a table. It notifies to said user terminal as an IP address of the terminal in a connection place network. It permutes by the address which changes into the IP address by which the connection place network distributed the transmitting agency address of the going-up packet addressed to a connection place network to this user terminal from a user terminal, and does not have said duplication. By two or more routing table The correspondence procedure by the VPN selection connection gateway characterized by choosing two or more roots which became independent logically, and sending out this packet.
[Claim 3] The VPN selection connection gateway characterized by to have a means to distribute an IP address to this user terminal that a user terminal starts in the VPN selection connection gateway according to claim 1 in addition to said each means, a means to offer GUI for changing a connection place network, the authentication means asked to RAS of a connection place network, and a means for making PPP connection.

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention is related in always-on connection mold access systems, such as ADSL, at the correspondence procedure by the VPN selection connection gateway and it which enable connection with NSP (Network Service Provider) of plurality [user terminals / in the same LAN / two or more / coincidence].

[0002]
[Description of the Prior Art] The ADSL (Asymmetric Digital Subscriber Line) technique which serves conventionally image transmission which coexisted with the telephone using the existing telephone line is known. For example, in the American telephone company, there is a video on demand which can call, view and listen to a movie etc. together with a call service using MPEG1 of an ADSL technique and digital image compression technology. On the other hand, the VPN service (Virtual Private Network Service) (virtual private network) attracts attention as service

which can use a public network like a dedicated network. Namely, subscriber's network can be used like an extension telephone in the company, for example, he sets up the telephone number of the arbitration of 2-7 figures, and can telephone now freely by the number. This is an entrepreneur (for example, NSP (Netwok Service Provider) has come out.) whom not only a voice network but the Internet provides with a VPN service.
[0003] Drawing 6 is always in the former the system configuration Fig. of a connection network. The system configuration of the network in always-on connection access systems, such as ADSL As shown in drawing 6 , it connects with the access network 9 via ADSL Modem (ATU-R) 2 from a user terminal 1-1 and 1-2. Furthermore, it connects with the core network 10 via DSLAM (Digital Subscriber Line Access Multiplexer (digital subscriber's-loop access multiplexer))3 and the ATM switch 4. It connects with the connection place NSP 5-1 and 5-2 via the ATM switch 4. ATU-R (ADSL Transceiver Unit-Remote (ADSL Modem of user ******))2 is equipped with an NAT function, DHCP server ability, and HTTP server ability as shown in 8. For example, in order to connect with the network 5 of NSP or Company LAN from a user terminal 1-1, from the ATM switch 4 on a core network, a user is set as the network which registered at the time of a contract fixed, and is connected to a contract network. The packet transmitted from the user terminal 1-1 passes along the ADSL network 9 from ATU-R2, and after termination of the 1 ** is carried out by DSLAM3, it is transmitted to the network concerned by the ATM switch 4.
[0004] In addition, the notation of each network node shown caudad is a protocol stack with which the node in the corresponding location is equipped, and shows the protocol conversion for every layer. In addition, when communicating using TCP/IP, a DHCP (Dynamic Host ConfigurationProtocol) server needs to set ADORE of an IP address, or the default and the gateway as a computer, and registers an IP address and the address of a default gateway on the DHCP server as a protocol for automating this. Moreover, a HTTP (Hyper Text Transfer Protocol) server is a server equipped with the protocol used in order to transmit and receive information, such as a WWW browser and a file. With such a configuration, since it is set as the network which registered at the time of a contract fixed, two or more user terminals cannot connect to a network different, respectively two or more networks which a user wishes not to mention the ability not to choose by on demand one, either.
[0005]
[Problem(s) to be Solved by the Invention] As mentioned above, by always-on connection access systems, such as the conventional ADSL, since it will connect with the network which registered at the time of a contract fixed, there was a problem that a connection place could not be chosen or it could not connect with the company or NSP which chooses a connection place as coincidence with two or more terminals, and is expected of it.
[0006] Then, the purpose of this invention solves the technical problem of these former, and is in the online communications using always-on connection access systems, such as ADSL, to offer the correspondence procedure by the VPN selection connection gateway and it which can realize service (it is hereafter described as a coincidence selection connection service) which selection (it is hereafter described as a selection connection service) of a connection place on demand and two or more computers by the side of [LAN] a user connect to two or more NSP and coincidence.
[0007]
[Means for Solving the Problem] In order to attain the above-mentioned purpose, the VPN selection connection gateway of this invention The DNS function to detect address solution and address duplication as equipment installed in a user side, The Twice-NAT function to change the

transmitting agency address (SA) and the transmission place address (DA), A virtual router (VR) function with two or more router ability which became independent logically, Detecting IP address duplication to a connection place network by having a DHCP function, HTTP server ability, and a RadiusClient function furthermore, and combining these Conversion of DA when there are SA of a transmission place IP packet and duplication is also performed, and routing of the packet is carried out to the demanded connection place NSP using VR chosen on the basis of SA of a user terminal. Thereby, it becomes possible to connect with two or more connection places arbitrarily at coincidence, permitting duplication of the IP address of PC in Connection NSP with User PC.

[0008]

[Embodiment of the Invention] Hereafter, a drawing explains the example of this invention to a detail.

(The 1st example) Drawing 1 is the system configuration Fig. of network configuration showing the 1st example of this invention, and drawing 2 is the explanatory view of the packet processing of VSG (VPN Selection Gateway) in drawing 1 . In the 1st example, the case where VSG6 and ADSL Modem (ATU-R) 2 are formed separately is shown, and both are not unified like the 2nd example. As are shown in drawing 1 and the 1st example shows to the preceding paragraph story of ADSL Modem (ATU-R) 2 of the access network 9 81, they are a Twice-NAT function, VR function (virtual router ability), DNS (domain Name System Server) server ability, DHCP server ability, HTTP server ability, and Radius. It is characterized by installing VSG6 equipped with the Client function. In addition, a DNS server is a server which performs address solution, and with NAT of Twice-NAT, fundamentally, although Private<-->Grobal is changed, Twice-NAT changes only SA (Source Address) not only about SA but about DA (Distination Address). In the case of NAT, the address space of a connection place assumes the Global thing. When the connection place uses the private address in the company [LAN] etc., the private address space and the conflict by the side of the inside LAN of ** may be started. Therefore, not only about SA but about DA, address translation is performed and the address is made not to carry out a conflict. The DNS (Domain Name System) function could set up the logical group who calls it a domain hierarchical, and incorporates and uses for a part of identifier of a computer the domain name which is a logical group name in the TCP/IP network. The DNS server has the conversion table of a host name and an IP address. Moreover, Radius Client (Remote Authentication Dial-in User Service Client) compares with the managed table of User Information the user ID and the password which are sent via an access server, and tells the propriety of authentication to an access server. This server is an administrative server of granting the access permission of an application server for every user, or collecting accounting information.

[0009] Drawing 1 shows the example for which a personal computer PC 1-1 communicates with PC (illustration abbreviation) of NSP#1, and PC 1-2 communicates with PC (illustration abbreviation) of NSP#2. Therefore, in order to offer two or more coincidence selection service, it is necessary to stretch two or more PPP sessions, therefore L2TP is used. PPP (Point to Point Protocol) is a protocol for WAN used when connecting and carrying out data communication of for two points. VR is chosen by SA and the IP packet sent by the user PC 1-1 is changed into the address to which the private address assigned by the DHCP server was assigned from NSP using the NAT function. When duplication of the connection place PC and an IP address is detected by the DNS server, it changes also about DA. The changed packet is transmitted to NSP through the appointed VC (Virtual Channel). When other users PC do a connection request to other NSP in parallel to this, in order to check SA and to choose different VR, it enables two or more PCs to

connect with coincidence at two or more NSP.
[0010] Drawing 2 shows the condition that packet processing for coincidence selection connection is performed, in VSG. It is the DHCP server ability and Radius by which 6 was mounted in VSG and 6-1 to 6-4 was mounted in VSG6 in drawing 2 . A Client function, HTTP server ability, and DNS server ability are shown. 6-5 to 6-9 is a reference table in VSG, and is the table 6-5 corresponding to SA-VR, VR (virtual router) 6-6, an address translation table (private side) 6-7, an address translation table (global side) 6-8, and the ARP table 6-9 at a detail. BAS (Bradband Access Server) which is an access server for 6-10 to hold L2TP and for 7 hold not only dialup but ADSL and ATM is shown. An injection of the power source of PC 1-1, 1-2, and 1-3 acquires an IP address from the DHCP server 6-1 of VSG. In addition, let the IP address which a DHCP server gives to PC 1-1, 1-2, and 1-3 be the private address of the class of the arbitration set to RFC1918 here.
[0011] Drawing 3 is the sequence chart of the VPN selection connection gateway which shows the 1st example of this invention of operation. PC 1-1 requires an IP address of DHCP beforehand (101), and acquires an IP address from the DHCP server 6-1 (102). PC 1-1, 1-2, and 1-3 connect with the HTTP server 6-2 using a web browser (103). The connection place NSP is chosen from a server 6-2 by (104) and GUI (Graphical User Interface) by an NSP selection screen being displayed (105 (VR decision)). A user name and a password are entered and it is Radius. It attests by sending out an authentication demand to the authentication server of the connection place NSP which Client 6-3 chose (106) (108). In addition, authentication actuation is asked to RAS (Remote Access Srver (equipment which holds a dialup user and transmits a packet to a core network)) of a connection place network. When a user's authentication is performed, VR name for Connection NSP matched with SA of the sending-out packet of PC is set as the selection VR name field of the table 6-5 corresponding to SA-VR (109). For example, it is changed into SA:a->VR name:VR1 at SA:b->VR name:VR2, respectively. The address translation table 6-7 which matches the IP address (Ga) assigned to coincidence from the NSP side and the private address (a) currently assigned to PC 1-1 is generated (110). About PC 1-2, it generates similarly. The ARP table 6-9 which matched the IP address and MAC Address of PC is generated from the processing of an ARP table which PC 1-1 and 1-2 performed (111).
[0012] Next, the procedure with which PC 1-1 sends out an IP packet to NSP#1 is described. In order that PC 5-1-1 of NSP#1 and PC 1-1 which communicates may solve the IP address from the identifier of PC 5-1-1, the query packet (answerback to a Request packet) of DNS is transmitted to the DSN server 6-4 of VSG6 (112). VSG6 acts as the forward of the DNSquery from PC 1-1 to DNS server 5-1-2 of the connection place NSP 5-1 specified by VR 6-6-1 (113). The IP address (a') of PC 5-1-1 is returned as response from the DNS server of the DNS server of NSP#1 to PC 5-1 (114). In addition, 'a' and 'a" are the same IP addresses. However, both the IP addresses of PC 1-1 and PC 5-1 are set to 'a' here, and duplication occurs. Then, DNS server 5-1-2 changes the IP address (a') of PC 5-1-1 into the address (germanium) of other arbitration, and adds the mapping to the address translation table (global side) 6-8 of VR 6-6-1 (115).
[0013] Thus, the response packet of changed DNS is transmitted to PC 1-1 (116). Now, in PC 1-1, the IP address of PC 5-1-1 is remembered to be 'Ga'. From now on, the IP packet transmitted to PC5from PC 1-1-1-1 will be transmitted as SA:a and DA:germanium. Suitable VR is chosen from SA of a packet in VSG6, and the transmitted packet performs conversion of both SA and DA (117,118). That is, it is changed into SA:a->Ga and DA:germanium->a'. By this conversion, a packet passes along PPP#1, using the L2TP tunneling 6-10 as a thing addressed to Address germanium, and is sent out to the core network 10 via DSLAM3 and BAS7 (refer to drawing 1).

Attachment 3 (Reference 2)

[0014] The packet (119) sent out from PC 5-1-1 of NSP#1 is sent out to VSG6 through PPP#1, and conversion of SA and DA is performed in VSG6 (120). (SA:a'->germanium, DA:Ga->a) And with reference to the ARP table 6-9, it is transmitted to PC 1-1 (121). PC 1-2 is able to perform NSP#2 and a communication link to coincidence. PC 1-2 should choose NSP#2. All the tables were set up as shown in the sequence chart of drawing 4 , and in the transmit data from PC 1-2 and other PCs, since Selections VR differ, as for PC 1-1, the sending-out place VC (Virtual Channel) has been independent. Therefore, the problem that the sending-out data from PC 1-1 and the sending-out data from PC 1-2 are mixed up is not produced.
[0015] (The 2nd example) Drawing 4 is the network block diagram showing the 2nd example of this invention, and drawing 5 is always using VSG which built in the ATU-R function drawing of a connection ADSL network in drawing 4 . In addition, at this example, although PPPoverATM is used, it can carry out similarly by IPoverATM. The 2nd example shows the case where VSG6a of a configuration of having unified VSG and an ATU-R function is used (82 reference of drawing 4). In this case, since there is no constraint by the interface between VSG and ATU-R unlike the 1st example, a direct packet can be transmitted to the ATM interface of ADSL. That is, since Plurality VC (Virtual Channel) was stretched, as drawing 1 showed, in order to stretch two or more PPP sessions on ATM, it is not necessary to use a L2TP protocol. Moreover, the ATU-R function 6-11 is arranged instead of L2TP 6-10 in drawing 2 also about the configuration in VSG of drawing 5 . The other configuration is almost the same. Although it is the same as the 1st example shown in drawing 3 about the sending-out processing sequence of an IP packet, the sending-out place VC (Virtual Channel) is described by VR (virtual router), and it differs at the point transmitted to BAS7 via IP packet VC.
[0016]
[Effect of the Invention] According to [as explained above] this invention, they are DNS server ability, HTTP server ability, and Radius. Since address duplication of NSP connected the user side LAN by preparing the VPN selection connection gateway which mounted a Client function, DHCP server ability, and a SA+VR routing function does not occur, it enables two or more computers to connect with two or more NSP at coincidence.

[Brief Description of the Drawings]
[Drawing 1] It is always which shows the 1st example of this invention the block diagram of a connection ADSL network.
[Drawing 2] It is the detail block diagram of VSG in drawing 1 .
[Drawing 3] It is a sequence chart of operation by the ADSL network which shows the 1st example of this invention.
[Drawing 4] It is always which shows the 2nd example of this invention the block diagram of a connection ADSL network.
[Drawing 5] It is the detail block diagram of VSG which built in the ATU-R function in drawing 4 .
[Drawing 6] It is always in the former the block diagram of a connection network.
[Description of Notations]
1-1, 1-2, 1-3 -- User PC, 5-1-1 -- PC of NSP, 2 -- ATU-R (ADSL Modem), 3 -- DSLAM, 4 -- ATM switch (exchange), 5-1, 5-2, 5-3 [-- VPN selection connection gateway (VSG),] -- NSP, 6 -- VSG, 7 -- 81 BAS, 82 9 [-- HTTP server ability,] -- An access network, 10 -- A core network, 6-1 -- DHCP server ability, 6-2 6-3 -- Radius A Client function, 6-4 -- DNS server ability, 6-5 [-- An address translation table (global side), 6-9 / -- An ARP table, 5-1-2 / -- DNS server by the

English translation of Document 1

Hajime Umemoto, "BSD de My Server o Tsukuro! , Dynamic Tunnel"

Page 115 – Page 117

By the way, fixed IPv4 global addresses are required for establishing a tunnel. This means that no IPv6 tunneling can be achieved under the environments of dialing, CATV, etc. in which IPv4 addresses are dynamically assigned.

As one of the methods for solving this problem, Trumpet Company proposed DTCT (Dynamic Tunnel Configuration Protocol).

In DTCT, which is a protocol using IPv4 TCP, the server side dynamically sets a tunnel for Ipv4 addresses of the client at a request for connection from the client side. In addition, a system similar to APOP is used for authentication.

Here, an IPv6 over IPv4 tunnel cannot exceed IPv4 NAT basically. Attention is called to the fact that DTCP is not something that clears this constraint.

A distribution kit of KAME includes DTCP server and client described in Ruby, and can be used if Ruby is installed.

However, although KAME is integrated in recent BSD, DTCP server and client are not attached. They may be taken from the distribution kit of KAME and used with slight modifications.

DTCP has "Host" and "Tunnelonly" as types of tunnel.

"Host" is a type in which only a single IPv6 address is assigned. It may be likened to dialing with PPP (Fig. 1).

"Tunnelonly" is used only for establishing a tunnel, and does not make any assignment of IPv6 address or route control. It may be easily understood if we say that it performs "gifconfig" only as command. Assignment of IPv6 address and route control are made separately either by manual operation or by using a route control daemon, etc. (Fig. 2)

With the use of DTCP, a "host" type tunnel can be operated easily. However, this is not interesting because it is no different from what is done by freenet6.

It would be better to assign a prefix of IPv6 to sites where IPv4 addresses are not fixed.

"Tunnelonly" type is used to that purpose, but it does not work so well. Because, with the use of DTCP, the state of gif interface dynamically changes, it becomes necessary for the route control daemon to be capable of following that change. However, "Zebra" which we are using cannot follow changes in the interface. For that reason, no route information flows even if a tunnel is newly established.

Furthermore, with dialing, the link remains established indefinitely if there is a flow of route control protocol, and this is uneconomical and requires some special consideration in the operation.

To solve this problem, we added a tunnel-type "tunnelroute", by modifying "dtcps/drcpc" attached to KAME. (Note 3)

This consists in preparing a database of IPv6 addresses assigned to the respective users on the server side and, when a tunnel is set, performing static routing in response to the connected users (Fig. 3).

With DTCP, a recovery of tunnel is made, in case of disconnection of

IPv4 or non arrival for a specific time of keep-alive message. This is enough with "host" or "tunnelonly." With "tunnelroute," however, no immediate reconnection can be made in case the tunnel became unusable for reasons such as dynamic changes of IPv4 address, etc., because the route information remains valid during the waiting for time-out.

To avoid this problem, it is so arranged that any remaining route information may be deleted, in case there is a request for reconnection from the same user.

DTCP uses a method conformable to APOP for authentication. With mounting of KAME, the user DB is directly diverted from "popper," and the user registration is made with a "popauth" command.

A DTCP user may not necessarily be a UNIX account, but needs to be registered in "/etc/passwd" with a dummy, because any non-registered user is not accepted by "poopauth."

After the registration, operation can be made with "tunnelonly" type by simply starting "dtcps."

When approving a "host" type tunnel, you specify the prefix of the IPv6 address to be assigned to the argument of "dtcps."

To approve "tunnelroute" type, prepare "/usr/local/v6/etc/routetable." "routetable" is a pair of user name and assigned IPv6 prefix (List 1).

"dtcps" searches and uses an empty gif interface. This presents some slight inconvenience in the case of presence of a static tunnel and, for that reason, a modification is made so that the scope of gif interface used by "dtcps" may be specified optionally for practical use. "dtcps" calls out commands such as "gifconfig," etc., and attention must be paid to the path so

that a command correctly adapted to IPv6 may be called out.

List 2 shows examples of starting script in the case of IPv6 tunneling realized by using KAME.

Attachment 5 (Reference 3)

Eiji YAMADA, "Solution Unyo Kokoga Point! Dai 1 kai, Internet VPN Unyo-zenpen Pilot Test to Sekkei no Point", N+1 NETWORK, Softbank publishing Inc., Vol. 2, No. 12, 01 December, 2002 (01. 12. 02), pages 130 to 135, 'IP Address no Unyo' Ran

Almost all Internet VPN operations involve workarounds, except operations accompanying environmental changes such as the addition of rules. Therefore with respect to the content of this series, I will provide understanding from such points of view as workaround-conscious verification methods and operations. First of all, I shall start by providing points to note on designing and verifying. This is because many failures arise from insufficient verification at the design and pilot test stages prior to the introduction of technology.

Considerations When Introducing IPsec

IPsec builds a secure tunnel among equipment. IPsec performs negotiations in the preliminary stage of establishing the tunnel, has a mutual table to maintain this state after establishment, and further, updates the tunnel periodically. Thus, IPsec may differ from ordinary communication equipment in that opposed equipment constructs and maintains a specific relation. That is, in IPsec operations, you must always be conscious of the other side as well as of yourself. Also, IPsec is susceptible to impacts from external factors such as line conditions in that it continues to operate by repeating negotiations such as updating the tunnel or cipher key. We should fully understand these circumstances specific to IPsec and carry out system design and pilot tests for long-term operation.

The following list shows key topics that you should consider and notice when deploying IPsec.

- Quality and amount of traffic
- Impact on the existing network
- Throughput and performance
- SA verification
- Router setting on the route

- IP address operation
- Mixed communication with plain and encrypted text
- Fragmentation
- Preferred authentication method
- Notes on combination with NAT
- Notes on combination with firewalls
- Notes on combination with other solutions
- IPsec client specification
- Management features
- Workaround
- Notes concerning export regulations
- Maintenance system

I recommend you consider these topics before your purchase. Now, in keeping with the theme of the series, this section describes matters among those given above concerning IPsec operation.

● Quality and Amount of Traffic

As long as IPsec is a kind of communication equipment, you should deploy it based on understanding of the amount and quality of traffic on the network to which IPsec is applied. The amount of traffic may vary over time, so you should have an understanding of the time zone in daily tasks when traffic reaches its maximum value, and of the host or segment where traffic converges most, and you should select a product in conformity to this flow. Also, in terms of traffic quality, we should pay attention to the flowing packet size and application timeouts. As IPsec performs processing such as encryption processing and header addition internally, its overhead is large compared with the router. Figure 1 shows a test example of IPsec gateway performance from a certain manufacturer, and short packet processing gave a remarkably bad result. That is, like VoIP and streaming applications, there are products weak in processing consecutive short packets. Also, periodical tunnel updates are a feature specific to IPsec. In this feature, negotiations are performed

between equipment when updating and in the meantime, real data does not flow. Depending on the number of tunnels, it can take several minutes to do all of these updates so you should be careful if you are running an application that may time out. For the points to remember described here, you can do trial calculations based on information taken from the catalog specs and the manufacturer, but it is still preferable to perform a pilot test using actual machines, including the application environment.

● SA Verification

SA (Security Association) is a very important element for IPsec. SA refers to the state where, after a negotiation between IPsec devices, both parties set various parameters such as cryptographic and hash algorithms and the cipher key on their SA tables to be ready for encrypted communication. SA is a highly influential factor at the operational stage as well as at the Internet VPN design stage. First, at the design stage, equipment is selected corresponding to network scale, but note that for the SA upper limit value, diverse expressions such as "number of tunnels" and "number of sessions" are used according to each manufacturer. SA, as you may know, is established by a procedure called IKE (Internet Key Exchange) between devices, and two types of SAs exist: phase 1 SA (ISAKMPSA) and phase 2 SA (IPsec SA). As shown in Figure 2, a phase 1 SA is established between devices, that is against the other, so it is affected by the number of sites, and phase 2 SA is built based on targets such as hosts which perform cipher communication or subnet, so it is affected by the network scale. Also, as for phase 2 SA, two connections to the opposed target are set up in two directions according to each security protocol (AH or ESP), and moreover as shown in Figure 3, the next SA is provided a little before the update time limit in order not to break the communication, so double phase 2 SAs are held for a certain period of time. However, as for the numerical value provided by the manufacturer, it would often be ambiguous whether it indicates phase 1 or phase 2 SA, or whether it is based on duplicated phase 2 SAs. As the SA upper limit value can affect not only the design stage but also later extensions, you should survey it steadily. It can be effective to perform the pilot test in SA on the expected scale, but as you would have to prepare as many devices as the number of opposed targets, it is hard to realize the pilot test on phase 1 SA. Therefore, it is

realistic to get definite information from the manufacturer and to carry out a flexible design based on the numerical values. Also, as mentioned above, SA has a time limit (Life Time), being updated periodically. It is a tunnel update, and it is also the timing of cipher key update. As IPsec repeats updating SA all the time while operation, the setting for SA Life Time in the dial-up or DSL environments such as mobile or ISDN requires some amount of caution. In the DSL-based Internet VPN as recently increased examples, a fixed address is assigned from ISP to the center site where the server is set up, and the branch site with terminal only often uses the service for obtaining an address dynamically. In this case, as the target (or tunnel point) IP address for the branch site side may differ each time the line is reconnected, the center side cannot start the IPsec connection as a sender. For the same reason, the IKE negotiation for updating SA should be started from the branch side. Therefore, in the example as mentioned above, you should set the SA Life Time for the branch site side to a shorter value than that for the center side to get the IKE process started from the branch side intentionally. In particular, if you set up the IPsec device from the different manufacturer at the opposed site, you might want to test in the live environment whether the operation meets your expectations. In the test, make the SA Life Time as short as possible to cause the SA to update frequently. You might want to check whether communication can be maintained without any problem for several hours.

Furthermore, an SA recovery procedure during failure may significantly affect subsequent operations. For example, if the device A is rebooted due to a power outage or failure while SA is established between IPsec devices A and B, SA table of the device A will be cleared but the SA information concerning the device A remains in the table of the opposed device B. In this condition, if the device A tries to reconnect after the reboot, the device B will not negotiate with it as it still has old SA information. The SA recovery procedure in this case may differ according to product implementations. For some products, if it fails to negotiate several times, SA clear (DelSA) command is sent from the device A of the rebooted side to the device B where the SA still remains to forcibly erase the SA, and the device B initiates the IKE negotiation again to rebuild SA. Whereas for a product from another manufacturer, if a negotiation fails, the device B, where the SA still remains, erases it spontaneously,

and accepts a new negotiation from the device A. If you use a product from manufacturers with different SA recovery procedure as an opposed device, the SA may not be recovered automatically when a failure occurs. If the SA Life Time expires, the SA can probably be rebuilt, but if the time limit is set to several hours, the communication can disrupt in the meantime. Therefore, in case of combinations without automatic recovery, if the one is rebooted, you should be informed about it, and you should reboot the opposed device manually. However, although one-to-one VPN may bring a satisfactory construction, but VPN construction among multiple sites may bring about just a troublesome problem. As shown in Figure 4, suppose that the IPsec device A on the center site is building VPN with devices B, C, and D on branch sites, and the device A is provided by distinct manufacturer from that of devices on other sites, so you should recover the SA manually. If the device B is rebooted due to a power outage, you should reboot the device A to recover the SA between devices A-B. However, if the device A is rebooted, SA information concerning C and D in the device A will be erased, so next you should reboot devices C and D before you rebuild the SAs between A-C and A-D. That is, in this example, a reboot at one site can cause reboots at all sites. In order to build VPN between products from different manufacturers, you should test by reproducing the real environment using multiple devices. You might want to write recovery procedures including human procedures beforehand based on confirmed behaviors thereby. By the way, there are products with the function to select and delete specific SA information only, by installing such product on the center site, you can erase only the SA on the site that requires rebooting and be ready for reconnection.

● Router Setting on the Route

IPsec uses the UDP port number 500 for exchanging IKE. Also, it uses specific protocol numbers such as IP type number 51 for AH and IP type number 50 for ESP. In addition, IPsec can use a specific port for management depending on the products. If there is a spot where these ports are closed on the route for building VPN, IPsec VPN cannot be established.

As is sometimes the case, filtering is set on the firewall established in networks such as

CATV or on the router rented from ISP, and ports necessary for IPsec operation are closed. You need to check with your provider beforehand that the necessary ports are open.

● IP Address Operation

Basically, IPsec describes VPN rules using IP addresses, so you should pay attention to IP address operations. Almost all IPsecs may be used in tunnel mode in the Internet VPN, but then, hosts in each site connected with VPN communicate mutually using private addresses. (Except when a global address is assigned to each host). As private addresses within the same corporate location may be kept in good condition, they cannot be duplicated, but in case of connecting to other corporate locations such as in electronic commerce, address systems can happen to duplicate each other. In such a case, settle the problem by assigning a global address to the public server, or in case of an IPsec device with NAT capability, by converting it into a global address with NAT.

You should also pay attention to IP address operations in mobile environments. The PC in a mobile environment communicates using global addresses dynamically allocated by ISP, but the site installed in the server may require routings according to its network configuration. In this case, treatment such as allocating private addresses within the site temporarily to the mobile terminal may be required. In order to meet these requests, each IPsec product begins to implement the capability of assigning an address to the mobile terminal on its own. Ipsec-OHCP is now on the way to standardization as such a capability. Ipsec-OHCP uses a process whereby the IPsec device on the site receives and relays the communication from the mobile terminal implemented with IPsec client software, and passes a private address retrieved from the DHCP server on the internal LAN to the mobile terminal. Also, the process another implementation uses has the IPsec device on the site keep several private addresses pooled beforehand and the IPsec device itself assigns the address to the mobile terminal. In both cases, if several hundred mobile terminals may try to connect simultaneously, an address space suitable for this number of terminals should be prepared. Depending on circumstances, you should reconstruct the address system in the site.

● Preferred Authentication Method

In IPsec, you can use PKI (Public Key Infrastructure) or RADIUS authentication as extended functions in addition to authentication options such as Pre Shared Key authentication, digital signature authentication, and public key authentication, and particularly on the operational side, you should be careful when using PKI. PKI responds diversely according to IPsec products, and initial authentication, certificate abolishment procedures or the like may differ according to IPsec products. The most commonly used procedure is for the certificate issue request in PKCS 107 format to be carried out from the IPsec device side and a certificate in PKCS #7 format to be issued from the PKI side, but there is no specific unified method for passing formats. Some pass the data offline, while others pass the data online using a Web browser as an interface, like SCEP (Simple Certificate Enrollment Protocol). Also, you can import the certificates beforehand into IC cards, and then replace the certificate issue by distributing the IC cards to the users. In all events, when using PKI, you should establish a procedure for issuing certificates in preparation for real operation. Also, when operating CRL (Certificate Revocation List), the VPN communication may stop by failing the CRL update due to communication failure or the like. When using PKI, you should check operations relevant to PKI other than IPsec operation in a pilot test beforehand, such as by checking the behavior or error message when a problem occurs in CRL operation.

● Notes on Combination with NAT

The most significant reason why a corporation deploys an Internet VPN is the reduction of communication costs. Recently, I experienced an example of a certain user with 250 local sites who has migrated from frame relay to ADSL Internet VPN. The user did a trial calculation that showed a reduction of several tens of millions of yen in communication costs a year. The NAT router is often used for ADSL and when a configuration to implement IPsec client software in each terminal under the router is employed, the communication will of necessity traverse NAT. Whereas, as is well known, IPsec protocol with only standard functionality cannot traverse NAT. However, the use of NAT is increasing as ADSL diffusion grows. Several

technologies to traverse NAT based on these needs are proposed, and at present, the implementation of NAT-Traversal in many products is increasing. NAT-Traversal traverses NAT by encapsulating the IPsec traffic in UDP packet with source port number 500. Recently, products able to use any UDP or TCP port may have emerged. In the sense that these technologies are now on the way to standardization, if you employ the configuration through NAT, you need to test it on an actual machine beforehand and check its operation.

- Notes on Combinations with Firewalls

Although many recent firewall products implement IPsec, there may be a demand to definitely distinguish firewalls from VPN security policy or to keep firewalls separate from IPsec gateways for throughput reasons or the like.

There may be three main types of locations for installing both devices, as shown in Figure 5.

Suppose that a firewall divides global and private addresses using NAT and so on, the configuration (a) causes the problem of NAT traversal. Also, as encrypted packets pass over the firewall, high-precision access control is impossible. Therefore, usually we do not employ the configuration (a).

In configuration (b), as packets sent from the internal LAN are processed by NAT before passing the IPsec gateway, the problem of NAT traversal never arises. Also, packets sent from the Internet pass the firewall after decryption, so full access control is possible.

In configuration (c), as the firewall and IPsec gateway are on separate routes, they do not interfere with each other. This configuration is appropriate if you want to change the existing firewall setting as little as possible. However, the internal router or the like should carry out routing such that it allows "this packet to pass through the firewall and that packet to pass through the IPsec gateway" according to the destination addresses of packets sent from the internal LAN. In this manner, as each configuration has advantages and disadvantages, select one according to your required specifications.

- Management Feature

Attachment 5 (Reference 3)

Items to be managed in order to operate IPsec are as follows:

- Policy management
- SA management
- Error log management

First, for policy management, IPsec should have functions to register and manage the settings necessary for IPsec construction such as rule management, which host or subnet will start to build the VPN for example, preferred authentication method, and IKE parameter setting, and distribute them to each device. Although IPsec uses the management tool provided by the manufacturer for concrete operations, recently, they often use the Web browser as an interface. The user interface may differ completely depending on the product, in particular, the ways of distributing policy to the IPsec clients may be various, such as some centralizing distribution on a directory basis, while others send the policy by file to each PC and make each user set the policy. In order to save the trouble of operation, you need to examine beforehand which method should be employed.

In IPsec, in case of trouble, first check the SA state. SA management function may differ according to the user interface and so on. One IPsec collects all SA states of each device, another logs-in and checks for each device, and another manages all devices from the SNMP server by providing the extended MIB. Manual SA deletion, as mentioned above, may differ depending on the product, such as some will erase all SAs together, while others can delete specific SAs selectively.

Basically, the logs of error or the like are obtained by the management tool provided by the manufacturer, while some products support Syslog and collect logs using an external management server. Also, others connect to each device via serial cable or the like directly and log locally. The log content may differ according to the product, but almost all products issue typical error messages in case of trouble, and only a few messages indicate the failure cause directly. Therefore, you should evaluate comprehensively by checking not only error messages, but the records of the SA state before the failure occurrence and communication state obtained from SA management or Syslog. When carrying out the SA recovery test of an IPsec device as mentioned

above, additionally checking what types of records are recorded to various logs and what types of error messages are recorded, may be helpful for real operation in future.

Need for Pilot Testing

In the description above, I have explained the need for a pilot test beforehand in some cases. In summary, the implementation of some IPsec features may differ depending on the product so desk check only is insufficient. In particular, in heterogeneous connections where products from various manufacturers are mixed, or in cases of applying relatively new technologies such as ADSL, you should carry out a pilot test. When carrying out a pilot test, having applications and product construction as close as possible to the same environment as the real operation will probably give the most accurate results.